



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/655,230	09/05/2000	Chung Nan Chang	2170	7762
7590	06/14/2005		EXAMINER	
Donald E Schreiber Donald E. Schreiber A Professional Corp. Post Office Box 2926 Kings Beach, CA 96143-2926			KIM, JUNG W	
			ART UNIT	PAPER NUMBER
			2132	

DATE MAILED: 06/14/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Advisory Action Before the Filing of an Appeal Brief	Application No. 09/655,230	Applicant(s) CHANG, CHUNG NAN
	Examiner Jung W. Kim	Art Unit 2132

--The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

THE REPLY FILED 01 June 2005 FAILS TO PLACE THIS APPLICATION IN CONDITION FOR ALLOWANCE.

1. The reply was filed after a final rejection, but prior to or on the same day as filing a Notice of Appeal. To avoid abandonment of this application, applicant must timely file one of the following replies: (1) an amendment, affidavit, or other evidence, which places the application in condition for allowance; (2) a Notice of Appeal (with appeal fee) in compliance with 37 CFR 41.31; or (3) a Request for Continued Examination (RCE) in compliance with 37 CFR 1.114. The reply must be filed within one of the following time periods:

- a) The period for reply expires 3 months from the mailing date of the final rejection.
 b) The period for reply expires on: (1) the mailing date of this Advisory Action, or (2) the date set forth in the final rejection, whichever is later. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of the final rejection.

Examiner Note: If box 1 is checked, check either box (a) or (b). ONLY CHECK BOX (b) WHEN THE FIRST REPLY WAS FILED WITHIN TWO MONTHS OF THE FINAL REJECTION. See MPEP 706.07(f).

Extensions of time may be obtained under 37 CFR 1.136(a). The date on which the petition under 37 CFR 1.136(a) and the appropriate extension fee have been filed is the date for purposes of determining the period of extension and the corresponding amount of the fee. The appropriate extension fee under 37 CFR 1.17(a) is calculated from: (1) the expiration date of the shortened statutory period for reply originally set in the final Office action; or (2) as set forth in (b) above, if checked. Any reply received by the Office later than three months after the mailing date of the final rejection, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

NOTICE OF APPEAL

2. The Notice of Appeal was filed on _____. A brief in compliance with 37 CFR 41.37 must be filed within two months of the date of filing the Notice of Appeal (37 CFR 41.37(a)), or any extension thereof (37 CFR 41.37(e)), to avoid dismissal of the appeal. Since a Notice of Appeal has been filed, any reply must be filed within the time period set forth in 37 CFR 41.37(a).

AMENDMENTS

3. The proposed amendment(s) filed after a final rejection, but prior to the date of filing a brief, will not be entered because
 (a) They raise new issues that would require further consideration and/or search (see NOTE below);
 (b) They raise the issue of new matter (see NOTE below);
 (c) They are not deemed to place the application in better form for appeal by materially reducing or simplifying the issues for appeal; and/or
 (d) They present additional claims without canceling a corresponding number of finally rejected claims.

NOTE: _____. (See 37 CFR 1.116 and 41.33(a)).

4. The amendments are not in compliance with 37 CFR 1.121. See attached Notice of Non-Compliant Amendment (PTOL-324).

5. Applicant's reply has overcome the following rejection(s): _____.

6. Newly proposed or amended claim(s) _____ would be allowable if submitted in a separate, timely filed amendment canceling the non-allowable claim(s).

7. For purposes of appeal, the proposed amendment(s): a) will not be entered, or b) will be entered and an explanation of how the new or amended claims would be rejected is provided below or appended.

The status of the claim(s) is (or will be) as follows:

Claim(s) allowed: _____.

Claim(s) objected to: _____.

Claim(s) rejected: _____.

Claim(s) withdrawn from consideration: _____.

AFFIDAVIT OR OTHER EVIDENCE

8. The affidavit or other evidence filed after a final action, but before or on the date of filing a Notice of Appeal will not be entered because applicant failed to provide a showing of good and sufficient reasons why the affidavit or other evidence is necessary and was not earlier presented. See 37 CFR 1.116(e).

9. The affidavit or other evidence filed after the date of filing a Notice of Appeal, but prior to the date of filing a brief, will not be entered because the affidavit or other evidence failed to overcome all rejections under appeal and/or appellant fails to provide a showing of good and sufficient reasons why it is necessary and was not earlier presented. See 37 CFR 41.33(d)(1).

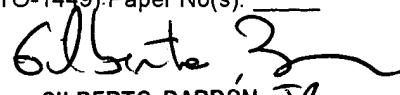
10. The affidavit or other evidence is entered. An explanation of the status of the claims after entry is below or attached.

REQUEST FOR RECONSIDERATION/OTHER

11. The request for reconsideration has been considered but does NOT place the application in condition for allowance because:
See Continuation Sheet.

12. Note the attached Information Disclosure Statement(s). (PTO/SB/08 or PTO-1449). Paper No(s). _____

13. Other: _____.

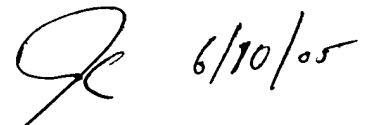

GILBERTO BARRON JR.
 SUPERVISORY PATENT EXAMINER
 TECHNOLOGY CENTER 2100

Continuation of 11. does NOT place the application in condition for allowance because: In reply to applicant's remark that "the preceding logical proof' irrefutably proves that the plurality of public quantities is not stored by the sender and hence claim 40 is not covered by the prior art of record (pg. 6, 1st full paragraph), it is noted that applicant's main premise of the "logical proof" is based on a supposition that is not valid. On pgs 2-3, Applicant argues that the plurality of public quantities are stored in one of three places and only one of the three places: the sender, the receiver or a trusted third party. ("[o]nly one (1) of the three (3) preceding summary declarations can be true", pg. 3, 2nd paragraph, last sentence). Applicant's rational for this supposition is that the plurality of public quantities can only be established by one of the three entities (pg. 5, 1st full paragraph) and further points to Crandell that the public values are established by a third part (pg. 3, last paragraph). However, the step of establishing the pluraltiy of public quantities and the step of storing the plurality of public quantities are two distinct steps; the "logical proof" is an argument that is not directed to the issues of the recited claim.

Moreover, regarding applicant's allegation that the Crandell reference does not disclose or even suggest comparing the results obtained by evaluting expressions of at least two different verification relationships, and hence does not cover the limitations of claim 40 (pgs. 29-30), the Crandell disclosure is quite clear, the limitation is met by the cited reference. If applicant desires the limitation of the two independent verification relationships as expressed on pg. 22, line 6-24, line 13, then such a limitation must be recited in the claims. Otherwise claim interpretation is based on a broadest resonable interpretation (MPEP 2111).

In reply to applicants argument that Hellman does not teach all the limitations of claim 27, specifically that the elements of a plurality of sender's quantities from the sending cryptographic unit and the at least some of the pluraltiy of public quantities are not taught, the values are in fact all disclosed: the public quantities q and a covers the at least some of the plurality of public quantites and the y1 covers the plurality of sender's quantities (Hellman, fig. 1 and col. 8:37-49; the variation using m-dimensional vector space defines a plurality of quantities for each of q, a and y1).

Finally, in reply to applicant's argument that Schneier adds nothing to the disclosure of Hellman et al., examiner disagrees since an explicit disclosure of a disinterested public repository and the role of the repository clearly teaches the limitation of a public repository for storing public quantities of the cryptographic system and further establishes several objectives as a set forth in Graham v. John Deere Co., 383 U.S. 1, 148 USPQ 459 (1966), specifically resolving the level of ordinary skill in the pertinent art and considering objective evidence present in the application indicating obviousness or nonobviousness.

A handwritten signature consisting of a stylized 'J' or 'R' followed by the date '6/10/05'.